Opis przedmiotu

Nazwa przedmiotu: Bezpieczeństwo systemów i sieci komputerowych

2. **Kod przedmiotu: 11.3 SSK.BSS.06**

3. **Język wykładowy**: polski

4. **Kierunek**: Informatyka

5. **Specjalność**: Systemy i sieci komputerowe

6. **Rok**: 3 Semestr: 6

7. **Tytuł/stopień oraz imię i nazwisko prowadzącego przedmiot**:

dr inż. Mariusz Gola

8. **Tytuły/stopnie oraz imiona i nazwiska pozostałych członków zespołu**:

……..

9. **Formy zajęć wchodzące w skład przedmiotu, wymiar godzinowy, forma zaliczenia**:

Forma zajęć	Wykład	Ćwiczenia/ Ćwiczenia tablicowe	Laboratorium/ Ćwiczenia praktyczne	Projekt	Seminarium
Liczba godzin w semestrze	30		15		
Forma zaliczenia	Egzamin testowy		Średnia z ocen cząstkowych		

10. **Liczba punktów ECTS**: 3

11. **Poziom** : zaawansowany

12. **Wymagania wstępne**:

Podstawowe wiadomości z zakresu systemów operacyjnych i technologii sieciowych.

13. **Cele kształcenia**:

Celem zajęć jest zapoznanie studentów z podstawowymi problemami bezpieczeństwa systemów informatycznych. Wykład obejmuje zagadnienia związane z zagrożeniem poufności, integralności i dostępności informacji, modele bezpieczeństwa i klasy bezpieczeństwa systemów informatycznych, bezpieczeństwo protokołów komunikacyjnych, elementy kryptografii i zagadnienia związane z podpisem elektronicznym i infrastruktura klucza publicznego. Wyjaśnione zostanie pojęcie polityki bezpieczeństwa i sposób jej definiowania, dobrych praktyk, monitorowania, zarządzania bezpieczeństwem i audytu.

14. **Opis treści kształcenia w ramach poszczególnych form zajęć**:

14.1. **Wykład**:

- Wstęp - przestępstwa komputerowe, normy i zalecenia, polityka bezpieczeństwa
- Zagrożenia i mechanizmy ochrony. Źródła zagrożeń. Aspekty prawne i organizacyjne. Uwierzytelnianie, autoryzacja, kontrola dostępu
- Dostępność usług i jej zwiększanie.
- Bezpieczeństwo systemów operacyjnych. Naruszenia bezpieczeństwa, najczęstsze zagrożenia
- Bezpieczeństwo sieci. Bezpieczeństwo protokołów, usług i urządzeń sieciowych. Tunelowanie. Zapory sieciowe. monitorowanie, NAT, IDS/IPS. bezpieczeństwo infrastruktury sieci bezprzewodowych.
- Kryptografia: szyfry symetryczne, szyfry asymetryczne, podpis cyfrowy, infrastruktura klucza publicznego
- Zarządzanie bezpieczeństwem

14.2. **Ćwiczenia/Ćwiczenia tablicowe**:

14.3. **Laboratorium/ Ćwiczenia praktyczne**:

W ramach laboratorium studenci będą nabywać praktycznych umiejętności związanych z wykorzystaniem usług ochrony stosowanych w systemach i sieciach komputerowych:

1. Wykorzystanie oprogramowania do szyfrowania i ukrywania informacji 4h
2. Praktyczne aspekty wykorzystania certyfikatów i struktury PKI 2h
3. Monitorowanie przewodowej i bezprzewodowej sieci komputerowej 4h
4. Implementacja i administracja firewall'a na wybranej platformie 5h

15. **Literatura podstawowa**:

1. Maiwald E. *Bezpieczeństwo w sieci*. Kraków: Wydawnictwo Edition2000 2002
2. Molski M., Opala S. *Elementarz bezpieczeństwa systemów informatycznych*. Warszawa: Mikom 2002
3. Pipkin D. L. *Bezpieczeństwo informacji. Ochrona globalnego przedsiębiorstwa*. Warszawa: WNT 2002

16. **Literatura towarzysząca**:

1. RSA Security. *A Guide to Security Policy*. Bedford, MA, USA, 2000
2. Wallace Wang "Internet, hakerzy, wirusy", RM 2001
3. Joel Scambray, Mike Shema "Hakerzy - Aplikacje webowe", Translator 2002
4. Rob Flickenger "100 sposobów na sieci bezprzewodowe", Helion 2004